Team Name: f0gd0gs

Results Email: [redacted]

Examination Time Frame: April 14, 2008 to Oct 29, 2008

204 Steganography Level 2

Methodology:

Steganography is a difficult problem space. We used several detection tools in an effort to limit the endless possibilities of "rabbit holes" that we might chase down. Essentially, we used publically available tools in order to get direction. In the end, Stegdetect while old and historically not particularly useful proved to be very useful in this particular case. Short execution remarks found below.

StegSpy 2.1
no results for any files.

XStegsecret
no results for any files.

StegalizerSS v3.1
File 1 shows some indication of have LSB encoded data.

Stegdetect 0.6
File 3 : appended (3250) <[random][data][7z..'….XL&U..]>

Stegbreak 0.6
no results for any files.

Answers:

File3 contains a 7zip archive starting at 0x2934E. This 7zip archive can be opened by any uncompressor that supports the 7zip format. The 7zip archive contains one file: mirage.bmp. This picture is of a several cars in a parking lot (one of them is a mirage) and an African American man getting into a red Mitsubishi Eclipse (or Eagle Talon) coupe. The image is in the recovered directory for challenge 204 on the media accompanying this report and can be seen below:

The 7zip file can be extracted using dd:

```
#>dd if=File3.jpg of=file3.7z bs=1 skip=168782
```

The 168782 is simply the starting offset (0x2934E) in decimal.

Tools used:
Type: specialized steganography detection software
Name: StegSpy
Publisher: Bill Englehardt
Compiled (free)
Site: http://www.spy-hunter.com/stegspydownload.htm

Type: specialized steganography detection software
Name: xstegsecret
Publisher: Alfonso Munoz
Open Source
Site: http://stegsecret.sourceforge.net/
Note: requires java (jre), and the GUI is in Spanish.

Type: specialized steganography detection software
Name: StegalizerSS
Publisher: SARC
Commercial (free trial – registration required)